Pour citer cet article : Marx J, et al. L'hôpital attaqué. Presse Med Form (2024), 10.1016/j.lpmfor.2024.04.003

Presse Med Form 2024; xx: xxx

en ligne sur / *on line on*
www.em-consulte.com/revue/lpmfor
www.sciencedirect.com

L'hôpital attaqué

Julien Marx [1], Christophe Leroy [2], Jean-Marc Philippe [3], Benoît Vivien [4]

Disponible sur internet le :

1. Conservatoire national des Arts et Métiers, équipe sécurité et défense - renseignement, criminologie, crises, cybermenaces (ESDR3C), Paris, France
2. Assistance publique–Hôpitaux de Paris, Direction qualité partenariat patient - DPQAM, service de gestion des crises sanitaires - SSE, Paris, France
3. Ministère de la santé et de la prévention, Direction générale de la Santé, Paris, France
4. Hôpital universitaire Necker - Enfants malades, Assistance publique - Hôpitaux de Paris et université Paris Cité, société française de médecine de catastrophe, SAMU de Paris, service d'anesthésie-réanimation, Paris, France

Correspondance :
Benoît Vivien, Hôpital universitaire Necker-Enfants malades, Assistance publique–Hôpitaux de Paris et Université Paris Cité, SAMU de Paris, Paris, France.
benoit.vivien@aphp.fr

Points essentiels

L'hôpital, de par ses missions de santé auprès des populations, présente toutes les caractéristiques des cibles vulnérables : un rôle essentiel pour la nation, mais une accessibilité extrême pour tous types d'agressions et menaces, endogènes, exogènes, naturelles, technologiques, et bien sûr terroristes.
L'hôpital et les services de secours sont loin d'être épargnés par des attaques terroristes, mettant en jeu divers types d'armes le plus souvent conventionnelles, parfois avec des attaques secondaires ou l'utilisation d'ambulances comme vecteurs piégés.
Les attaques directes de l'hôpital faisant appel à des agents nucléaires, radiologiques (NR) et chimiques (C) sont bien plus rares, et l'hôpital n'est généralement que la victime secondaire, fortuite ou préméditée, d'un événement chimique extrahospitalier accidentel ou terroriste.
La menace la plus prégnante à ce jour est en pratique représentée par les cyberattaques, qui non seulement provoquent une désorganisation massive et durable du système hospitalier, mais peuvent être à l'origine d'une morbi-mortalité immédiate par la paralysie de systèmes de monitorage ou de suppléance vitale de patients de soins critiques.
La réponse à ces différents types de situations sanitaires exceptionnelles passe désormais par le dispositif ORSAN, cadre intégré de préparation et de montée en puissance des établissements et professionnels du système de santé.

Key points

The hospital attacked

The hospital, through its health missions to populations, presents all the characteristics of vulnerable targets: an essential role for the nation, but an extreme accessibility for all types

of aggressions and threats, endogenous, exogenous, natural, technological, and of course terrorists.
The hospital and emergency services are far from being spared from terrorist attacks, involving various types of weapons, most often conventional, sometimes with secondary attacks or the use of ambulances as booby-trapped vectors.
Direct attacks on the hospital using Nuclear, Radiological agents (NR) and Chemical (C) agents are much rarer, and the hospital is generally only the secondary victim, fortuitous or premeditated, of an accidental or terrorist extra-hospital chemical event.
The most significant threat to date is in practice represented by cyber-attacks, which not only cause massive and lasting disorganization of the hospital system, but can be the cause of immediate morbidity and mortality through the paralysis of monitoring or life support systems for critical care patients.
The response to these different types of exceptional health situations now involves the ORSAN system, an integrated framework for preparing and ramping up health system establishments and professionals.

Glossaire

C	**Chimique**
GTD	**Global Terrorism Database™**
NR	**nucléaire, radiologiques**
NRCB	**nucléaire, radiologique, biologique et chimique**
ORSAN	**Organisation de la réponse du système de santé**
RGPD	**règlement de la régulation générale de protection des données**

Introduction

L'hôpital, de par ses missions de soins, est en première ligne dès lors qu'il s'agit de prendre en charge des patients victimes d'agressions ou d'actes terroristes. Mais l'hôpital, et plus particulièrement ses services d'urgences tant intra-hospitaliers que pré-hospitaliers, peuvent également représenter les cibles directes ou indirectes, voire les vecteurs d'actions malveillantes ou criminelles. À ce titre, les établissements et structures de santé au sens large répondent aux caractéristiques de « cibles vulnérables » ou « cibles molles » telles que définies lors de l'Assemblée générale de l'ONU en 2006 [1]. D'une part, ils font partie des infrastructures critiques du pays puisque jouant un rôle capital dans la prestation d'un service essentiel, la préservation de la santé des populations, dont l'interruption risque de sérieusement compromettre la sécurité et le bien-être social et économique du pays, et à ce titre ils devraient être extrêmement sécurisés. Mais d'autre part paradoxalement, ils présentent également toutes les caractéristiques des « cibles molles » puisqu'ouvertes et accessibles au grand public 24 h/24, sans restriction d'accès [2].

Si la majorité des actes terroristes perpétrés à ce jour envers des hôpitaux ont fait appel à des armes conventionnelles, essentiellement lors d'explosions et de fusillades, il ne faut pas oublier les aspects nucléaires, radiologiques, biologiques et chimiques (NRBC), avec comme exemple princeps l'attaque au gaz sarin dans le métro de Tokyo en 1995, qui a été à l'origine d'une contamination secondaire massive des personnels de l'hôpital St-Luke [3,4].

Enfin, de manière relativement récente, l'hôpital doit également faire face à un nouveau type de menace de plus en plus fréquent, les cyberattaques, perpétrées par de multiples groupes ou organisations le plus souvent étrangers, et parfois directement soutenus par des états. Ces attaques, généralement sous couvert d'une demande de rançon, non seulement provoquent une désorganisation majeure et durable de l'établissement concerné, mais peuvent également engendrer un risque vital direct et immédiat pour les patients lorsqu'elles sont à l'origine de pannes ou dysfonctionnements sur des appareils de soins critiques tels que moniteurs ou respirateurs.

Nous n'abordons pas dans ce chapitre les risques classiques habituels des établissements de santé, tels que les incendies, inondations, pannes électriques ou d'approvisionnement en fluides médicaux, qu'ils soient d'origine endogène accidentelle ou au contraire la conséquence d'une agression ciblée d'origine malveillante, voire relevant directement d'un acte terroriste. Nous n'envisageons pas non plus l'agression de l'hôpital au sens d'un envahissement de bâtiments de soins à l'occasion d'un mouvement de foule ou de violence urbaine se propageant secondairement sur l'établissement.

Risque conventionnel

À partir de la Global Terrorism Database™ (GTD), base de données internationale en open source contenant des informations sur près de 200 000 événements terroristes survenus dans le monde depuis 1970, plusieurs publications ont récemment recensé les différents actes ayant concerné des établissements et services de santé [5–7]. Il faut signaler que cette base de données exclue du recensement d'une part les « simples agressions » sans caractère

Pour citer cet article : Marx J, et al. L'hôpital attaqué. Presse Med Form (2024), 10.1016/j.lpmfor.2024.04.003

terroriste, et à l'opposé d'autre part les actes de guerre perpétrés lors d'un conflit entre états belligérants.

Entre 1970 et 2020, entre 430 et 454 attaques terroristes (selon les publications), ont été identifiées envers des hôpitaux dans 61 pays différents [5–7]. Ces différentes attaques, quasi exclusivement perpétrées à l'aide d'armes conventionnelles, majoritairement des bombes, explosifs, armes à feu et armes blanches, ont été à l'origine selon les publications de 1291 à 1641 morts, et de 1921 à 2 746 blessés. Avec 179 attentats, le Moyen-Orient et l'Afrique du Nord ont été les régions du monde les plus touchées, suivies de l'Asie du Sud avec 125 attentats. La fréquence des attaques terroristes envers les hôpitaux a augmenté plus particulièrement au cours des deux dernières décennies, de manière bien plus importante que l'augmentation globale des actes terroristes contre tous les autres types de cibles, avec un pic de 41 attaques en 2014. Dans au moins trois événements, les hôpitaux ont été identifiés comme des cibles secondaires, faisant l'objet d'une attaque consécutive délibérée contre un hôpital, et ce après un incident primaire survenu ou provoqué en dehors de l'hôpital [5].

Parmi ces différentes attaques, 78 d'entre elles visaient une personne spécifique au sein de l'établissement, dont environ la moitié (52,6 %) impliquait un personnel médical. Les attaques envers des praticiens et soignants de soins primaires (médecins généralistes, etc.), au nombre de 29 colligées dans la GTD, ont été à l'origine de 58 décès, 52 blessés et 13 enlèvements ou prises d'otages [8].

Il faut également noter qu'une proportion importante de l'ensemble des attaques terroristes recensés dans la GTD visait des praticiens et/ou des établissements pratiquant des actes de soins spécifiques, en particulier des avortements. Au total, 262 attaques terroristes ont été identifiées dans cinq pays différents, dont la très grande majorité (96,6 %) aux États-Unis. Outre les 97 % de dommages matériels qu'ils ont provoqués, ces actes ont entraîné neuf décès et 34 blessés, et il faut également signaler trois enlèvements [9].

Considérant ces différents actes terroristes, les services d'urgences intra-hospitaliers et pré-hospitaliers représentent évidemment une cible privilégiée de par leur exposition et leur facilité d'accès. Schmeitz et al. ont ainsi identifié 184 attaques perpétrées contre des « *Emergency Medical Services* (EMS) », à l'origine de 748 décès (dont 69 assaillants) et 1293 blessés [5]. Ces attaques, plus fréquemment perpétrées à l'aide de bombes (n = 85), incluant des véhicules piégés, et par armes (n = 65), ont visé essentiellement des ambulances (n = 166), des hélicoptères (n = 7), voire directement les personnels (n = 11). Paradoxalement, ces chiffres montrent que les services d'urgences intra-hospitaliers sont rarement la cible directe de ces attaques, ce que confirment Jasani et al. qui ne trouvent que six attaques perpétrées directement au sein de ces services [10].

À côté des attaques envers les établissements et services de soins, il faut également individualiser, toujours d'après les données de la GTD, 42 attaques visant des équipes de secours pré-hospitalières et en particulier des pompiers, faisant 26 morts et 95 blessés. Elément notable, sur ces 42 événements, 12 (28,6 %) étaient des attaques secondaires, durant lesquelles les pompiers répondant à un premier événement étaient ensuite eux-mêmes visés sur le site même de leur intervention primaire. La méthode la plus courante pour les attaques primaires et secondaires était l'utilisation d'une bombe ou d'un explosif. Bien que ces attaques soient rares, elles mettent en évidence à la fois la valeur stratégique et la vulnérabilité vis-à-vis des attaques terroristes des équipes de pompiers, et plus généralement de tous les services de secours extrahospitaliers [10]. Enfin, dans certains cas, les ambulances étaient volées avec violence par les terroristes, pour être ensuite secondairement utilisées dans le but d'infiltrer des hôpitaux afin de perpétrer une attaque armée ou être directement utilisées comme véhicules piégés [11].

Risques nucléaires, radiologiques, biologiques et chimiques (NRBC)

L'hôpital peut également être exposé à différents risques dans le domaine NRBC : en premier lieu bien évidemment des risques épidémiques liés à sa fonction dans la société, mais également des risques d'accidents industriels chimiques ou radiologiques voire nucléaires. Il peut aussi être la cible d'une dissémination intentionnelle de différents types d'agents, biologiques, nucléaires, radiologiques ou chimiques.

Les conséquences de la propagation d'un agent infectieux transmissible entre humains peuvent être majeures sur le moyen-long terme, comme l'ont montré les différentes vagues de la pandémie Covid-19 qui ont considérablement impacté l'ensemble des structures hospitalières de par le monde. Nous ne détaillons pas dans ce chapitre les caractéristiques de ce type d'événement lié au risque B.

De même, considérant le risque radio-nucléaire, les événements extrahospitaliers restent heureusement extrêmement limités, hormis certains accidents majeurs survenus au sein de centrales nucléaires : Three Mile Island (1979), Tchernobyl (1986), et Fukushima (2011) [12]. Les conséquences pour l'hôpital dépendent évidemment de la cinétique et de l'ampleur de l'événement, et il reste difficile d'en édicter de grands principes, raison pour laquelle le risque nucléaire et radiologique (NR) n'est pas envisagé dans ce texte.

A contrario, les rapports concernant des événements de catégorie chimique sont bien plus nombreux, aussi bien liés à des événements industriels civils que des attaques terroristes ou étatiques. Lors d'un événement chimique extrahospitalier, un grand nombre de victimes valides vont se présenter spontanément et rapidement dans les établissements de proximité, exposant alors ces derniers au risque de contamination secondaire des personnels soignants, et d'incapacitation majeure de la structure de soins. Deux exemples classiques d'événements

permettent d'illustrer les conséquences de ce risque pour l'hôpital : l'explosion accidentelle de l'usine de Bhopal en 1984 en Inde, et l'attaque du métro de Tokyo par la secte Aum en 1995 au Japon.

Le 2 décembre 1984, une explosion est survenue dans une usine de pesticides de Bhopal (Inde), libérant près de 45 tonnes d'isocyanate de méthyle (MIC) sous la forme d'un nuage toxique sur la ville et en particulier sur un bidonville voisin. La fuite de ce gaz mortel plus lourd que l'air, donc diffusant près du sol, a été à l'origine d'une panique dans l'ensemble de la ville de Bhopal, et tous les hôpitaux ont été rapidement submergés [13]. Les médecins locaux ne disposaient d'aucune information sur la toxicité et sur l'épidémiologie de l'empoisonnement au MIC, et le seul traitement médical s'est limité à une prise en charge symptomatique des lésions. Si très peu de documents sont disponibles concernant la saturation des hôpitaux lors de ce qui est considéré comme la pire catastrophe industrielle de l'histoire, le nombre de victimes, avec 3500 décès lors des 24 premières heures, laisse imaginer l'ampleur des difficultés dans les établissements de santé, a fortiori dans un pays en voie de développement. Mais, même en France, pays industriel moderne, les deux événements marquants de ces deux dernières décennies que sont l'explosion de l'usine AZF à Toulouse, et l'incendie de l'usine Lubrizol à Rouen [14–16] doivent nous rappeler que nous ne sommes pas à l'abri de catastrophes technologiques pouvant avoir un retentissement hospitalier majeur. À ce titre, une explosion telle que celle survenue sur le port de Beyrouth en 2020 doit faire partie des hypothèses accidentelles envisageables en France [17].

Le 20 mars 1995, vers 7h55, un acte terroriste a été perpétré par la secte Aum Shinriky consistant en cinq attaques coordonnées sur les lignes du métro de Tokyo. Un membre de chaque équipe a percé avec la pointe d'un parapluie un sac posé au sol contenant des poches de sarin sous forme liquide, laissant le gaz s'évaporer et diffuser dans les cinq rames bondées à l'heure de pointe (8 heures du matin). L'hôpital de proximité St-Luke (capacité 520 lits) a été alerté à 8h16, et les premières ambulances sont arrivées à 8h43. Au total, ce sont près de 500 patients qui sont arrivés en une heure dans le service d'urgence, dont trois en arrêt cardio-respiratoire [3,18]. Le personnel de l'hôpital, porteur de gants et masques de soin standard, a été secondairement contaminé, et 110 personnels ont présenté des symptômes d'intoxications, mais aucun à un niveau sévère. Si les stocks d'antidotes étaient en quantité suffisante, le sarin n'a en revanche été formellement identifié que vers 11h00, après une fausse information initiale faisant état d'une intoxication à l'acéto-nitrile. Outre l'absence de tenues de protection adaptées, une zone d'accueil de capacité restreinte et mal ventilée, sans zone de décontamination pré-définie, l'absence de plan intra-hospitalier NRBC, ainsi que des problèmes de transmission, ont été les principales difficultés identifiées a posteriori lors de cet événement. Le bilan relativement limité de cette attaque chimique, avec un total de 13 morts et 6300 blessés, aurait été lié à la mauvaise qualité et à la dilution du sarin produit par les terroristes.

Une revue récente effectuée à partir de la GTD a permis d'identifier, entre 1970 et 2017, 383 actes terroristes ou de guerre faisant appel à un agent chimique, en particulier dans des zones de guerre comme la Syrie et l'Irak [19]. Parmi ceux-ci, il faut individualiser les attaques chimiques directes sur des hôpitaux, notamment en Syrie, et en particulier celle sur l'hôpital chirurgical de Latamneh, le 25 mars 2017. Alors que cet établissement avait été construit dans une grotte pour le protéger des frappes aériennes, plusieurs bombes ont été larguées par un hélicoptère sur l'entrée de l'hôpital. Bien que l'attaque n'ait causé que des dommages structurels mineurs à l'établissement, plusieurs sources à l'intérieur de l'hôpital ont déclaré qu'au moins une des bombes, qui ont atterri à l'intérieur de l'hôpital, contenait un agent chimique, ultérieurement confirmé par des experts médicaux comme étant du chlore [20,21]. Cette attaque avait causé la mort de deux membres du personnel, dont un des médecins de l'hôpital. D'autres attaques sporadiques sur des structures hospitalières ont eu lieu, mais restent peu documentées à ce jour. Néanmoins, il s'agit d'une menace réelle et sérieuse, à laquelle tous nos établissements de santé doivent dorénavant se préparer [22,23].

Risques « cyber »

L'évolution des technologies de l'information et le développement des systèmes d'information ont profondément modifié l'écosystème numérique des établissements de santé durant la dernière décennie. Le développement rapide de nouveaux outils et l'appropriation de ces technologies par les acteurs de la santé ont ouvert la voie à des approches modernes et facilité les échanges entre les professionnels, tant dans le domaine du soin que dans la gestion des fonctions supports. Mais cette digitalisation de l'hôpital a également induit une dépendance et créé de multiples vulnérabilités, et la maîtrise de ces nouveaux risques par les acteurs de terrain constitue par conséquent un chalenge face au niveau des différentes menaces possibles dans ce domaine.

À ce titre, la cyber-malveillance et les cyberattaques représentent incontestablement la nouvelle menace du XXI^{e} siècle, pour toutes les entreprises, sociétés ou établissements utilisant des systèmes informatiques et outils numériques, c'est-à-dire la quasi-totalité du monde du travail. Si la majorité des cibles est constituée d'entreprises ou de collectivités, les établissements de santé n'en représentent que près de 10 %. Mais en réalité, ces attaques d'établissements de santé sont le plus souvent fortuites, dans le sens où les hackers explorent de manière exhaustive des milliers de sites internet d'entreprises à la recherche d'une brèche de sécurité, et accèdent par hasard au système d'information d'un hôpital. C'est alors qu'ils évaluent plus précisément le type de cible qu'ils ont réussi à infiltrer, ainsi

Pour citer cet article : Marx J, et al. L'hôpital attaqué. Presse Med Form (2024), 10.1016/j.lpmfor.2024.04.003

que son pays d'origine, et consécutivement sa valeur marchande potentielle.

Les cyberattaques envers les établissements de soin, qui avaient pourtant bénéficié d'une certaine trêve de la part des cybercriminels durant le tout début de la crise COVID, se sont multipliées ces dernières années, passant en France de 392 en 2020 à 733 en 2021 [24]. Les hôpitaux représentent en effet des cibles toutes particulières pour les cybercriminels, qui vont infiltrer le système d'information de l'établissement à l'aide d'un *ransomware* ou « rançongiciel ».

Vol de données de santé

En premier lieu, il faut savoir que les données de santé sont catégorisées au sens du Règlement de la régulation générale de protection des données (RGPD) comme des « données sensibles », et tant la perte des données de santé pour l'établissement (et pour le patient), qu'a contrario la menace de leur divulgation au grand public, constituent un premier moyen de pression des hackers, généralement sous la forme de demande d'une rançon. Ces bases de données de dossiers de patients comportant des informations administratives mais également médicales, se négocient ensuite sur le *darkweb*, généralement en bitcoins pour des sommes équivalent à plusieurs centaines de milliers d'euros [25]. Ainsi, lors de la cyberattaque du centre hospitalier de Corbeil-Essonnes en août 2022, la demande de rançon aurait été de 10 millions de dollars de la part du groupe de hackers russes Lockbit 3.0, groupe qui a ensuite également été à l'origine quelque mois plus tard de l'attaque du centre hospitalier de Versailles. Si en France les établissements de santé, et plus généralement les organismes publics, ont une interdiction administrative de procéder à ce type de paiement, ce n'est pas le cas outre-Atlantique, où les établissements de santé sont privés et acceptent le plus souvent le paiement. Ainsi, aux États-Unis, près de 400 hôpitaux avaient été la cible d'une cyberattaque en 2020, avec des demandes de rançon de l'ordre de deux millions de dollars pour chacun d'entre eux, ce qui donne une estimation d'environ 1,3 milliards de dollars au total versés aux cybercriminels en 2021 [24].

Interférence avec le fonctionnement d'appareils biomédicaux

Le deuxième risque de ces cyberattaques envers des établissements hospitaliers est représenté par la possibilité d'interférer avec le fonctionnement d'appareils biomédicaux. En effet, la plupart de ces dispositifs sont connectés à internet, dans le but de permettre d'effectuer des maintenances et mises à jour à distance par les fabricants. Les systèmes informatiques des appareils de radiologie, de par leur haute technicité informatique, sont particulièrement identifiés par des hackers, qui peuvent ainsi accéder par ce tunnel à l'ensemble du réseau informatique de l'hôpital. Certains sites internet spécialisés (« Shodan ») permettent d'accéder à la liste de tous les appareils et dispositifs personnels et professionnels connectés sur internet. Si les logins et mots de passes sont inchangés par rapport à la version d'usine ou particulièrement simples (admin/1234), il devient alors aisé pour des hackers de pouvoir prendre le contrôle de cet appareil biomédical. De nombreux dispositifs peuvent par conséquent être perturbés dans leur fonctionnement dans les établissements de santé, ce qui est susceptible de mettre en jeu le pronostic vital des patients lorsque ces dispositifs sont utilisés dans des unités de soins critiques : appareils de radiologie, automates d'analyses, centrale de monitoring, respirateurs de réanimation, etc. Ceci peut alors conduire à procéder à l'évacuation entière d'une unité de soins critiques, comme ce fut le cas pour le service de réanimation néonatale du centre hospitalier de Corbeil-Essonnes en août 2022. Paradoxalement, les services disposant d'appareils anciens voire vétustes, non connectés à internet (dispositifs d'hémodialyse, etc.), restent technologiquement « protégés » vis-à-vis de ces cyberattaques, ce qui peut permettre au service de poursuivre son activité avec un fonctionnement relativement préservé, sous réserve du niveau de dépendance aux autres appareils de l'établissement (système d'information, laboratoire de biologie centralisé, etc.). Enfin, il faut également signaler que de multiples dispositifs biomédicaux individuels implantés (pompe à insuline, pace-maker, défibrillateur, etc.) sont également connectés à internet et représentent autant de cibles potentielles pour les hackers, aussi bien en établissement de santé que pour l'immense majorité des patients en ambulatoire [25].

Contre-mesures immédiates

Pour faire face à l'évènement « cyber », et tout particulièrement lors de sa phase initiale de chaos durant laquelle l'établissement et ses personnels sont face à un océan d'incertitudes, il faut pratiquement réapprendre l'hôpital de nos grands-parents, avec la pochette de dossier, les différentes fiches de prescription en couleurs, le carton de demande d'examens radiographiques. Cependant, ces contre-mesures doivent également être pensées avec le double objectif d'une part de pouvoir recollectionner des données lors de la phase de récupération, et d'autre part de pouvoir ultérieurement intégrer ces données papier dans le dossier numérique lors du retour à la normale.

Conclusion

L'hôpital, ouvert sur l'extérieur de par sa mission de soin au grand public, représente une cible vulnérable idéale pour toutes les actions malveillantes et terroristes, qu'elles soient directes indirectes, conventionnelles, NRBC ou informatiques. Chaque établissement doit donc se préparer à faire face non seulement à des situations sanitaires exceptionnelles classiques comme un afflux de victimes, une pandémie, ou plus simplement une panne électrique, mais également à de multiples risques polymorphes.

Cette anticipation passe bien sûr par la rédaction de plans permettant d'envisager tous les risques et situations possibles, mais surtout par la réalisation d'exercices de mise en situation réguliers, théoriques et pratiques, permettant de tester et adapter les différentes procédures mises en œuvre. La préparation aux situations sanitaires exceptionnelles, notamment à l'hybridation des menaces génératrices de scénarios complexes (ex. attentat avec nombreuses victimes et cyberattaque conjointe) doit également s'envisager non seulement à l'échelon de l'hôpital, mais plus largement d'un territoire voire d'une région.

C'est l'objet du dispositif ORSAN (Organisation de la réponse du système de santé), cadre intégré de préparation et de réponse du système de santé dont l'objectif est de pouvoir faire face à toute situation sanitaire exceptionnelle en organisant de façon coordonnée la mobilisation des professionnels de santé et la montée en puissance des opérateurs de soins. Cette réponse passe par la mise en œuvre de leurs plans respectifs de montée en puissance, comme par exemple le plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles des établissements de santé, ainsi que son volet numérique, l'ensemble étant couplé au plan de sécurisation de l'établissement [26,27].

Déclaration de liens d'intérêts : les auteurs déclarent ne pas avoir de liens d'intérêts.

Références

[1] Soixantième session de l'Assemblée générale de l'Organisation des nations unies. Résolution 60/288, Points 46 et 120 de l'ordre du jour: La stratégie antiterroriste mondiale des Nations Unies. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/504/89/PDF/N0550489.pdf?OpenElement. (accès le 9/1/2024).

[2] Protéger les cibles vulnérables contre les attaques terroristes. Guide de bonnes pratiques. Nations Unies, Bureau de lutte contre le terrorisme, 2022. https://www.un.org/counterterro@&rism/sites/www.un.org.counterterrorism/files/2118451_f_oct_vulnerable_targets_module_1_web.pdf. (accès le 9/1/2024).

[3] Matsui Y, Ohbu S, Yamashina A. Hospital deployment in mass sarin poisoning incident of the Tokyo subway system–an experience at St. Luke's International Hospital, Tokyo. Jpn Hosp 1996;15:67–71 [PMID: 10161859].

[4] Okumura T, Suzuki K, Fukuda A, Kohama A, Takasu N, Ishimatsu S, et al. The Tokyo subway sarin attack: disaster management, part 2: hospital response. Acad Emerg Med 1998;5(6):618–24. doi: 10.1111/j.1553-2712.1998.tb02471.x.

[5] Schmeitz CTJ, Barten DG, van Barneveld KWY, De Cauwer H, Mortelmans L, van Osch F, et al. Terrorist attacks against emergency medical services: secondary attacks are an emerging risk. Prehosp Disaster Med 2022;37(2):1–7. doi: 10.1017/S1049023X22000140 [Online ahead of print. PMID: 35105401].

[6] Ulmer N, Barten DG, De Cauwer H, Gaakeer MI, Klokman VW, Van der Lugt M, et al. Terrorist attacks against hospitals: world-wide trends and attack types. Prehosp Disaster Med 2022;37(1):25–32. doi: 10.1017/S1049023X22000012.

[7] McNeilly B, Jasani G, Cavaliere G, Alfalasi R, Lawner B. The rising threat of terrorist attacks against hospitals. Prehosp Disaster Med 2022;37(2):223–9. doi: 10.1017/S1049023X22000413.

[8] Wirken B, Barten DG, De Cauwer H, Mortelmans LJM, Tin D, Cals J. Primary care as primary target: a review of terrorist attacks against primary care providers and their offices. Prehosp Disaster Med 2022;37(4):451–4. doi: 10.1017/S1049023X22000954.

[9] Wirken B, Barten DG, De Cauwer H, Mortelmans L, Tin D, Ciottone G. Terrorist attacks against health care targets that provide abortion services. Prehosp Disaster Med 2023;38(3):409–14. doi: 10.1017/S1049023X23000341.

[10] Jasani G, Alfalasi R, Liang SY. Terrorist attacks against emergency departments. Am J Emerg Med 2023;64:43–5. doi: 10.1016/j.ajem.2022.11.011.

[11] Besenyo J, Barten DG, De Cauwer HG, Tin D, Gulyás A. A review of ambulance terrorism on the African continent. Prehosp Disaster Med 2023;38(2):237–42. doi: 10.1017/S1049023X23000213.

[12] Koyama A, Fuse A, Hagiwara J, Matsumoto G, Shiraishi S, Masuno T, et al. Medical relief activities, medical resourcing, and inpatient evacuation conducted by Nippon Medical School due to the Fukushima Daiichi Nuclear Power Plant accident following the Great East Japan Earthquake 2011. J Nippon Med Sch 2011;78(6):393–6. doi: 10.1272/jnms.78.393.

[13] Lorin HG, Kulling PE. The Bhopal tragedy-what has Swedish disaster medicine planning learned from it? J Emerg Med 1986;4(4):311–6. doi: 10.1016/0736-4679(86)90008-9.

[14] Dechy N, Bourdeaux T, Ayrault N, Kordek MA, Le Coze JC. First lessons of the Toulouse ammonium nitrate disaster, 21st September 2001, AZF plant, France. J Hazard Mater 2004;111(1–3):131–8. doi: 10.1016/j.jhazmat.2004.02.039.

[15] L'Hôpital de Rangueil au moment de la catastrophe de l'usine AZF. https://www.chu-toulouse.fr/l-hopital-de-rangueil-au-moment-de-la-catastrophe. (accès le 9/1/2024).

[16] Incendie de l'usine de Lubrizol: Surveillance du recours à la médecine d'urgence. Santé Publique France. Bulletin du 28/10/2019 (données au 27 octobre). https://www.santepubliquefrance.fr/regions/hauts-de-france/documents/bulletin-regional/2019/surveillance-des-recours-a-la-medecine-d-urgence-incendie-lubrizol.-point-au-10-octobre-2019.

[17] Iskandar N, Rahbany T, Shokor A. Healthcare and terrorism: the Lebanese experience. Disaster Med Public Health Prep 2022;16(3):1073–6. doi: 10.1017/dmp.2021.26.

[18] Okumura T, Suzuki K, Fukuda A, Kohama A, Takasu N, Ishimatsu S, et al. The Tokyo subway sarin attack: disaster management, part 2: hospital response. Acad Emerg Med 1998;5(6):618–24. doi: 10.1111/j.1553-2712.1998.tb02471.x.

[19] DeLuca MA, Chai PR, Goralnick E, Erickson TB. Five decades of global chemical terror attacks: data analysis to inform training and preparedness. Disaster Med Public Health Prep 2021;15(6):750–61. doi: 10.1017/dmp.2020.176.

[20] Elsafti Elsaeidy AM, Alsaleh OI, van Berlaer G, Alhallak AA, Saeed SS, Soliman A, et al. Effects of two chlorine gas attacks on hospital admission and clinical outcomes in Kafr Zita, Syria. Cureus 2021;13(8):e17522. doi: 10.7759/cureus.17522.

[21] Syrie : une attaque contre un hôpital soutenu par MSF fait plusieurs morts et blesses. https://www.msf.ch/nos-actualites/communiques-presse/syrie-attaque-contre-

hopital-soutenu-msf-fait-plusieurs-morts. (accès le 9/1/2024).

[22] Décret n° 2024-8 du 3 janvier 2024 relatif à la préparation et à la réponse du système de santé pour faire face aux situations sanitaires exceptionnelles. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000048851655. (accès le 15/1/2024).

[23] Guide d'aide à la préparation et à la gestion des tensions hospitalières et des situations sanitaires exceptionnelles au sein des établissements de santé. Ministère des Solidarités et de la Santé, 2019 (actualisation 2024). https://sante.gouv.fr/IMG/pdf/guide_situation_sanitaire_exceptionnelle.pdf. (accès le 9/1/2024).

[24] Baudoux N, Verboogen B. Cyberattaques : pourquoi les hôpitaux sont-ils des cibles de choix? L'Echo. 29 Septembre 2023. https://www.lecho.be/entreprises/cyberattaques-hacking-hopitaux.html#:~:text=Les%20h%C3%B4pitaux%20ont%20en%20leur,peuvent%20donc%20se%20revendre%20cher. (accès le 9/1/2024).

[25] Mennecier D. Cyberattaques et hôpital. Médecine de Catastrophe - Urgences Collectives 2020;4(4):327–30. doi: 10.1016/j.pxur.2020.06.006.

[26] Note d'information n° DGOS/PF/2023/94 du 15 juin 2023 visant à informer les établissements de santé de la publication d'un guide d'aide à la préparation au volet numérique du Plan blanc. https://sante.gouv.fr/fichiers/bo/2023/2023.12.sante.pdf#page=341. (accès le 15/1/2024).

[27] Instruction n° SG/HFDS/2016/340 du 4 novembre 2016 relative aux mesures de sécurisation dans les établissements de santé. https://www.legifrance.gouv.fr/circulaire/id/41530. (accès le 15/1/2024).